

I claim:

1 1. A method of assuring that a message sent to a
2 recipient was requested for opening by the recipient, the
3 method comprising:

4 encrypting a message using a session key to produce
5 an encrypted message;

6 encrypting the session key using a public key to
7 produce an encrypted session key;

8 generating a transaction identifier;

9 encrypting the transaction identifier to provide an
10 encrypted transaction identifier;

11 sending, by the sender, the encrypted session key
12 and the transaction identifier to an arbiter;

13 sending, by the sender, the encrypted message and
14 the encrypted transaction identifier to the recipient;

15 generating a request for the encrypted session key
16 based on the transaction identifier;

17 sending the request to the arbiter; and

18 generating, by the arbiter, evidence that the
19 request for the encrypted session key was received.

1 2. The method of claim 1 wherein the request comprises
2 the transaction identifier and said generating evidence
3 comprises logging that the transaction identifier was
4 received.

1 3. The method of claim 1 wherein the request comprises
2 the transaction identifier in unencrypted form such that
3 the arbiter does not perform any cryptographic operations
4 to extract the transaction identifier from the request.

1 4. The method of claim 1 wherein the arbiter does not
2 receive the encrypted message delivered from the sender
3 to the recipient.

1 5. The method of claim 1 further comprising notifying,
2 by the arbiter, the sender of the request.

1 6. The method of claim 5 wherein said notifying
2 comprises sending an e-mail to the sender.

1 7. The method of claim 1 wherein the request is
2 repeatedly transmitted for a predetermined period of time
3 by the recipient until the encrypted session key is
4 received.

1 8. The method of claim 1, further comprising:
2 signing the decrypted transaction identifier,
3 wherein said transmitting the request comprises sending
4 the signed decrypted transaction identifier to the
5 arbiter.

1 9. The method of claim 1 wherein said generating the
2 request comprises:

3 decrypting, using the recipient's private key, the
4 transaction identifier from the encrypted transaction
5 identifier to provide a decrypted transaction identifier;

6 signing the decrypted transaction identifier and a
7 nonce associated with that recipient; and

8 sending the signed decrypted transaction identifier
9 and the nonce to the arbiter.

1 10. A system to assure that a message was requested for
2 opening, comprising:

3 a sender to send encrypted decoding information and
4 an encrypted message;

5 an arbiter to store the encrypted decoding
6 information; and

7 a recipient to receive the encrypted message,
8 request the encrypted decoding information, decrypt the
9 encrypted decoding information and decrypt the encrypted
10 message using the decrypted decoding information;

11 wherein the arbiter, in response to receiving the
12 request, generates evidence that the request was
13 received.

1 11. The system of claim 10 wherein the sender also sends
2 a transaction identifier to the arbiter, the sender also
3 sending an encrypted transaction identifier to the
4 recipient, the transaction identifier being associated
5 with the encrypted decoding information, the arbiter

6 storing the associated transaction identifier and the
7 encrypted decoding information, wherein the recipient
8 decrypts the transaction identifier and requests the
9 decoding information using the transaction identifier,
10 and the arbiter returns the encrypted decoding
11 information associated with that transaction identifier
12 to the recipient.

1 12. A method of operating a recipient's messaging system
2 to assure that a message sent to a recipient was
3 requested for opening by the recipient, the method
4 comprising:

5 receiving an encrypted message that was encrypted
6 using a session key;
7 receiving an encrypted transaction identifier
8 associated with the encrypted message;
9 decrypting the transaction identifier;
10 generating a request for the encrypted session key
11 based on the transaction identifier;
12 sending the request to an arbiter;
13 receiving the encrypted session key;
14 decrypting the encrypted session key to provide a
15 decrypted session key; and
16 decrypting the encrypted message using the decrypted
17 session key.

1 13. A method of operating a sender's messaging system
2 to assure that a message sent to a recipient was
3 requested for opening by the recipient, the method
4 comprising:

5 encrypting a message using a session key to provide
6 an encrypted message;

7 encrypting the session key to provide an encrypted
8 session key;

9 generating a transaction identifier;

10 encrypting the transaction identifier to provide an
11 encrypted transaction identifier;

12 sending the encrypted transaction identifier and the
13 encrypted session key to an arbiter server;

14 sending the encrypted message and the encrypted
15 session key to a recipient; and

16 receiving a notification, from the arbiter, in
17 response to a request from the recipient for the
18 encrypted session key based on the transaction
19 identifier.

1 14. A method of operating a messaging system on an
2 arbiter server to assure that a message sent to a
3 recipient was requested for opening by the recipient, the
4 method comprising:

5 receiving a transaction identifier and an associated
6 encrypted session key;

7 receiving a request, from recipient, to send the
8 encrypted session key to that recipient, the request
9 comprising the transaction identifier;

10. returning, in response to the request, the encrypted
11 session key associated with the transaction identifier in
12 the request; and

13 generating evidence that the request to send the
14 encrypted session key was received.

1 15. A recipient's messaging system comprising:

2 a memory to store instructions and data;

3 a processor to execute the instructions stored in the
4 memory;

5 the memory to store:

6 an encrypted message that was received from a
7 sender;

8 one or more instructions to decrypt an encrypted
9 transaction identifier to provide a decrypted transaction
10 identifier;

11 one or more instructions to generate a request for
12 an encrypted session key based on the transaction
13 identifier;

14 one or more instructions to send the request to an
15 arbiter;

16 one or more instructions to receive the encrypted
17 session key;

18 one or more instructions to decrypt the encrypted
19 session key to provide a decrypted session key; and

20 one or more instructions to decrypt the encrypted
21 message using the decrypted session key.

1 16. A sender's messaging comprising:

2 a memory to store instructions and data;

3 a processor to execute the instructions stored in the
4 memory;

5 the memory to store:

6 one or more instructions to encrypt a message using
7 a session key to provide an encrypted message;

8 one or more instructions to encrypt the session key
9 to provide an encrypted session key;

10 one or more instructions to generate a transaction
11 identifier;

12 one or more instructions to encrypt the transaction
13 identifier to provide an encrypted transaction
14 identifier;

15 one or more instructions to send the transaction
16 identifier and the encrypted session key to an arbiter
17 server;

18 one or more instructions to send the encrypted
19 message, the encrypted transaction identifier and the
20 encrypted session key to a recipient; and

21 one or more instructions to receive a notification,
22 from the arbiter, in response to a request from the
23 recipient for the encrypted session key based on the
24 transaction identifier.

1 17. An arbiter comprising:

2 one or more instructions to receive a transaction
3 identifier and an encrypted session key; and

4 one or more instructions to receive a request, from
5 at least one recipient, to send the encrypted session key
6 to that recipient, the request comprising the transaction
7 identifier associated with that recipient.

1 18. The arbiter of claim 17 further comprising:
2 one or more instructions to return, in response to
3 the request, the encrypted session key associated with
4 the transaction identifier in the request.

1 19. The arbiter of claim 17 further comprising:
2 one or more instructions to generate evidence that
3 the request to send the encrypted session key was
4 received by matching stored transaction identifiers with
5 the transaction identifier from the request and logging
6 that the request was received.

1 20. An article of manufacture comprising a computer
2 usable medium having computer readable program code
3 embodied therein for assuring that a message sent to a
4 recipient was received by the recipient, comprising
5 instructions to:

6 encrypt a message using a session key to produce an
7 encrypted message;

8 encrypt the session key using a public key to
9 produce an encrypted session key;

10 generate a transaction identifier;

11 encrypt the transaction identifier to provide an
12 encrypted transaction identifier;

13 send the encrypted session key and the transaction
14 identifier to an arbiter;
15 send the encrypted message and the encrypted
16 transaction identifier to a recipient;
17 generate a request for the encrypted session key
18 based on the transaction identifier;
19 send the request to the arbiter; and
20 generate, by the arbiter, evidence that a request
21 for the encrypted session key was received.

1 21. The article of manufacture of claim 20 further
2 comprising instructions to notify the sender that the
3 request was received.

1 22. An article of manufacture comprising a computer
2 usable medium having computer readable program code
3 embodied therein for operating a recipient computer
4 system to assure a sender that a message sent to the
5 recipient was received by the recipient, comprising
6 instructions to:

7 decrypt an encrypted transaction identifier to
8 provide a decrypted transaction identifier;
9 generate a request for an encrypted session key
10 based on the transaction identifier;
11 send the request to an arbiter;
12 receive the encrypted session key;
13 decrypt the encrypted session key to provide a
14 decrypted session key; and

15 decrypt the encrypted message using the decrypted
16 session key.

1 23. An article of manufacture comprising a computer
2 usable medium having computer readable program code
3 embodied therein for operating a sender's computer system
4 to assure the sender that a message sent to a recipient
5 was received by the recipient, comprising instructions
6 to:

7 encrypt a message using a session key to provide an
8 encrypted message;

9 encrypt the session key to provide an encrypted
10 session key;

11 generate a transaction identifier;

12 encrypt the transaction identifier to provide an
13 encrypted transaction identifier;

14 send the encrypted transaction identifier and the
15 encrypted session key to an arbiter server;

16 send the encrypted message and the encrypted session
17 key to a recipient; and

18 receive a notification, from the arbiter, in
19 response to a request from the recipient for the
20 encrypted session key based on the transaction
21 identifier.

1 24. An article of manufacture comprising a computer
2 usable medium having computer readable program code
3 embodied therein for operating an arbiter computer system
4 to assure the sender that a message sent to a recipient

5 was received by the recipient, comprising instructions
6 to:

7 receive a transaction identifier and an encrypted
8 session key; and

9 receive a request, from at least one recipient, to
10 send the encrypted session key to that recipient, the
11 request comprising the transaction identifier associated
12 with that recipient.

1 25. The article of manufacture of claim 24 further
2 comprising one or more instructions to return, in
3 response to the request, the encrypted session key
4 associated with the transaction identifier in the request
5 to the recipient.

1 26. The article of manufacture of claim 24 further
2 comprising one or more instructions to generate evidence
3 that the request to send the encrypted session key was
4 received.